DLP

GOIT

DLP

Los sistemas DLP protegen los datos de las empresas identificando información confidencial y luego utilizando un análisis de contenido profundo para detectar y prevenir posibles fugas de información. Este análisis de contenido utiliza métodos como coincidencias de palabras clave, expresiones regulares y funciones internas para reconocer el contenido que coincide con la política de DLP de una empresa. Como resultado, las empresas pueden identificar, monitorear y prevenir automáticamente el robo o la exposición de datos protegidos.

DLP permite a las empresas:

- Identificar información confidencial en múltiples sistemas locales y basados en la nube
- Evitar el intercambio accidental de datos
- Supervisar y proteger los datos
- Eduque a los usuarios sobre cómo cumplir con las normas

El primer paso en la implementación de DLP es que las empresas definan los datos confidenciales que desean proteger y creen una política de DLP. Esto podría ser detalles de tarjetas de crédito, direcciones de correo electrónico y números de seguro social, o simplemente una lista de nombres en una hoja de cálculo.

Una política de DLP contiene:

- Ubicaciones y sistemas donde los datos deben protegerse
- Cuándo y cómo proteger los datos
- Reglas que definen acciones y datos confidenciales cuando se descubre un riesgo de seguridad
- Condiciones que asignan diferentes acciones a diferentes niveles de riesgo.

Tipos de amenazas de datos

Los cibercriminales una amplia gama de métodos de piratería que varían en simplicidad y sofisticación. Los tipos comunes de amenazas de datos incluyen:

- Extrusión- La extrusión es el acto de los cibercriminales que apuntan e intentan robar datos confidenciales. Intentan penetrar en los perímetros de seguridad de las empresas mediante técnicas como la inyección de código, el malware y el phishing.

- Amenazas internas- Una amenaza interna es una infracción que proviene del interior de una organización. La información privilegiada malintencionada podría ser un empleado actual o anterior, un contratista o un socio comercial que tenga información sobre las prácticas y los sistemas de seguridad de la organización. La información privilegiada abusa de sus propios permisos o compromete la cuenta de un usuario con privilegios más altos e intenta mover datos fuera de la organización.

DLP puede prevenir tales riesgos proporcionando a las empresas una visibilidad completa de las transacciones de archivos y la actividad de los usuarios en todo su entorno de TI. Permite a las empresas conservar archivos durante el tiempo que sea necesario para proteger los datos y los requisitos de cumplimiento, incluso cuando un empleado ha dejado la organización. La prevención de pérdida de

datos también permite capacidades de recuperación de archivos que permiten a las organizaciones recuperarse de pérdidas de datos accidentales o maliciosas.

- Exposición involuntaria- Las infracciones también pueden ser causadas por una exposición de datos no intencionada o negligente. Esto generalmente ocurre como resultado de procedimientos inadecuados de datos de los empleados, en los que los empleados pierden información confidencial o brindan acceso abierto a su cuenta o datos. También puede deberse a que las empresas no establecen las restricciones de acceso adecuadas en las políticas de la organización.

El motor de análisis de contenido de DLP permite a las empresas identificar cuándo la información confidencial corre el riesgo de ser compartida externamente. Luego, pueden tomar medidas registrando el evento para su auditoría, mostrando una advertencia al empleado que podría estar compartiendo la información sin querer o bloqueando activamente el correo electrónico o el archivo para que no se comparta.